Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

020.308 Out-Processing/Termination of Information Technology Personnel Policy

Version 2.4
April 5, 2019

Revision History

Date	Version	Description	Author
5/2/2005	1.0	Effective Date	CHFS IT Policies Team Charter
4/5/2019	2.4	Review Date	CHFS OATS Policy Charter Team
4/5/2019	2.4	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or delegate)	4/5/2019	Jennifer Harp	Jennifer Harp
CHFS Chief Information Security Officer (or delegate)	4/5/2019	Brian Lykins on behalf of Dennis Leber	Brian Lykins on behalf of Dennis Leber

Table of Contents

1 POLICY DEFINITIONS 4

2 POLICY OVERVIEW 6

2.1 Purpose 6
2.2 Scope 6
2.3 Management Commitment 6
2.4 Coordination among Organizational Entities 6
2.5 Compliance 6

3 ROLES AND RESPONSIBILITIES 7

3.1 Chief Information Security Officer (CISO) 7
3.2 Chief Privacy Officer (CPO) 7
3.3 CHFS OATS Information Security (IS) Team 7
3.4 Security/Privacy Lead 7
3.5 CHFS Contract, State, and Vendor Staff/Personnel 7
3.6 System Data Owner and System Data Administrators..7
3.7 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators 8
3.8 Kentucky Online Gateway (KOG) Service Requestor..8
3.9 CHFS Office of Human Resource Management (OHRM) Personnel Liaison 8

4 POLICY REQUIREMENTS 8

4.1 General 8
4.2 State Personnel: Resignation 8
4.3 State Personnel: Suspension/Administrative Leave..9
4.4 State Personnel: Termination 9
4.5 Contract Personnel 10

5 POLICY MAINTENANCE RESPONSIBILITY 10

6 POLICY EXCEPTIONS 11

7 POLICY REVIEW CYCLE..11

8 POLICY REFERENCES 11

1 Policy Definitions

- **Agency:** Defined by CHFS for the purpose of this document, agency or agencies refers to any department within CHFS.
- **Confidential Data:** Defined by the Commonwealth Office of Technology (COT) Standards Data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include: Data not releasable under the Kentucky State Law; Protected Health Information; Federal Tax Information; Social Security and Credit Card numbers
- **Contract Staff/Personnel:** Defined by CHFS as an employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Electronic Protected Health Information (ePHI):** Defined by the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule as individually identifiable health information, including demographic data, that relates to: the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. The13 individually identifiable health information items include many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- **Enterprise Identity Management (EIM):** Defined by the Enterprise Identity Management User Guide as the Commonwealth Office of Technology's (COT) solution for identity management for employees and other users in the Commonwealth. EIM is a centralized system designed to standardize account creation, modification, and removal for users in the Commonwealth. EIM manages Active Directory, Email, Skype/Lync, and Home Folder(s).
- **Federal Tax Information (FTI):** Defined by Internal Revenue Service (IRS) Publication 1075 as federal tax returns and return information (and information derived from it) that is in the agency's possession or control which is covered by the confidentiality protections of the IRC and subject to the IRC 6103(p) (4) safeguarding requirements including IRS oversight. FTI is categorized as Sensitive but Unclassified information and may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC 6103(p) (2) (B) Agreement.

FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

- **Personally Identifiable Information (PII):** Defined by KRS Chapter 61 House Bill 5 (HB5) and in accordance with NIST 800-53 Revision 4 as information which can be used to distinguish or trace the identity of an individual; person’s first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements: account number, credit card number or debit card number that in combination with any required security code, access code or password would permit access to an account; social security number, taxpayer ID number, driver's license number, state ID number, passport number or other ID number issued by the United States government, or individually identifiable health information, except for education records covered by The Family Educational Rights and Privacy Act of 1974 (FERPA).
- **Sensitive Data:** Defined by COT standards as data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include: All information identifiable to an individual including staff, employees, and contractors but not limited to dates of birth, driver’s license numbers, employee ID numbers, license plate numbers, and compensation information. The Commonwealth proprietary information including but not limited to intellectual property, financial data and more.\
- **Sensitive Financial Data (including PCI):** Defined by Payment Card Industry (PCI) Data Security Standards (DSS) Security Standards as cardholder and sensitive authentication data including Primary Account Number (PAN), cardholder name, expiration date, service code, full track data (magnetic stripe data or equivalent on a chip0, CAV2/CVC2/CVV2/CID, and PIN(s). CHFS also defines sensitive financial data anything that is inclusive of bank identification/information (i.e. bank routing number, account number, etc.).
- **State Staff/Personnel:** Defined by CHFS as an employee hired directly through the state within the CHFS.
- **Third Party**: Defined by CHFS as any contracted or government organization that is not a part of the agency’s organizational structure. This may include state or federal auditing agencies, state approved security contract vendors or other external organization whose capabilities can be determined sufficient to conduct assessment needs.
- **Vendor Staff/Personnel:** Defined by CHFS as an employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must implement a comprehensive level of security controls through an out-processing/termination policy. This document establishes the agency's Out-Processing/Termination of Information Technology (IT) Personnel Policy to manage risks and provide guidelines for security best practices regarding staff being dismissed or leaving a project/state employment.

2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 CHFS OATS Information Security (IS) Team

The CHFS OATS IS Team is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required.

3.4 Security/Privacy Lead

Individuals are designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of PII, ePHI, FTI and other financial sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS IS Team is responsible for the adherence of this policy.

3.5 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency’s applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.6 System Data Owner and System Data Administrators

Management/lead, or appointed delegate, who works with the application’s development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

3.7 Kentucky Online Gateway (KOG) Enterprise Identity Management (EIM) Administrators

Authorized KOG personnel are responsible for taking electronically submitted service requests received by KOG and submitting them to the Commonwealth Service Desk (CSD) for completion. These authorized staff personnel are responsible for basic validation of service request information and are listed as an approved IT service contact to submit service desk tickets for CHFS. Questions in regards to or for the KOG EIM Administrators can be submitted to the CHFSServiceRequests@ky.gov mailbox.

3.8 Kentucky Online Gateway (KOG) Service Requestor

A CHFS division director approved and appointed designated individual(s) that have the KOG Request application ability to submit service requests through KOG for user access. This individual(s) manages approved provisioning and de-provisioning of user(s) access to the following: Active Directory (AD), Application, Virtual Private Network (VPN), Home Folder, Shared Folder, Telephone, Enhanced Mailbox, Account, Skype for Business, Other. KOG Service Requestor must validate all KOG required user and billing code information obtained for the CHFS personnel requesting services.

3.9 CHFS Office of Human Resource Management (OHRM) Personnel Liaison

A CHFS approved and appointed designated OHRM individual(s) to submit requests through the Kentucky Human Resource Information System (KHRIS) for state CHFS staff.

4 Policy Requirements

4.1 General

This policy outlines guidelines regarding how CHFS handles departure or termination of all CHFS IT employees. Contracted technical personnel, are subject to greater scrutiny apart from CHFS state employees. IT personnel have a level of access to Cabinet IT resources that require additional cautions. This policy will outline the measures to be taken when a termination notice is received.

All exit procedures for state personnel can be found on the Office of Human Resource Management (OHRM) Exiting Employees (for Supervisors) Checklist. All IT staff must comply with this policy and all related OHRM procedures.

4.2 State Personnel: Resignation

When an IT state employee submits their resignation the designated OHRM personnel liaison will submit a request in KHRIS for network, application, and service access to be

revoked. It is the responsibility of the manager/supervisor, or designee, to follow exit procedures and determine the timeline by which the employee will transition their tasks to a successor.
The applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). In case the employee is leaving state government altogether, the manager/supervisor, or designee, would confer with the second level manager/supervisor in making this determination.

If the manager/supervisor, or designee, need access to the employee's mailbox they must submit an approved/signed COT Email Review Request (COT-F084) Form to the CHFSServiceRequests@ky.gov mailbox. If the manger/supervisor, or designee, need access to the employees file shares (i.e. shared folders, U: Drive, etc.) they must submit an approved Staff Service Request Form, EZ Version (COT-F181EZ) to the CHFSServiceRequests@ky.gov mailbox. Any employees who have EAS Domain accounts (i.e. Developers, Admin Accounts, etc.) the manager/supervisor, or designee, must submit an approved Staff Service Request (COT-F181) Form the CHFSServiceRequests@ky.gov mailbox to terminate these accounts.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information that could be exploited by departed employees.

4.3 State Personnel: Suspension/Administrative Leave

When an employee is suspended or placed on administrative leave, their network accounts must be disabled immediately during the suspension/leave period. The designated OHRM personnel liaison, must update the employee's suspension/administrative leave in KHRIS. If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 4.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information that could be exploited by departed employees.
Once the employee returns to work, the designated OHRM personnel liaison, must update the employees account in KHRIS to request the accounts be enabled. The OHRM Personnel Procedures Handbook – 4.1 Disciplinary/Corrective Action must be followed.

4.4 State Personnel: Termination

Should a situation arise where an employee who has merit status is being terminated and has been issued intent to dismiss letter, all access must be revoked/terminated. At the time the intent is issued, any administrative rights, as well as all other access must be removed. If the applicable supervisor deems the employee a risk to Commonwealth assets, they, or the designated service requestor, must update KHRIS to remove all rights and privileges for that employee immediately.

Once the decision has been made to terminate an employee, the applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). The terminated employee is prohibited from having any unsupervised access to the network. If it is determined that the former employee is to be allowed to recover email messages, addresses, or any personal documentation, the immediate supervisor will remain with that employee until the task is complete. If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 4.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information that could be exploited by departed employees.

4.5 Contract Personnel

When a contractor departs, their state manager/supervisor, or designated service requestor, must update the Kentucky Online Gateway (KOG) to immediately revoke all rights and privileges. Once the decision has been made to terminate a contract employee, the applicable manager/supervisor, or designee, must determine the state owned devices/resources that must be recovered (i.e. access badge, laptop computer, keys, etc.). If the manager/supervisor, or designee, need access to the employee's mailbox, file shares, or EAS Domain accounts, follow the process detailed in Section 4.2 above.

CHFS OATS IS Team recommends the responsible supervisor, or designee, notify appropriate technical or application personnel to update non-expiring account information that could be exploited by departed employees.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

Any application or services that are not currently housed within KOG must follow agency processes/procedures for appropriate removal of all employee access upon departure from employment.

7 Policy Review Cycle

This policy is reviewed at least annually and revised on an as needed basis.

8 Policy References

- Approved OATS Service Requestors List
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Form: E-mail Request Form, COT-F084 Form
- Enterprise IT Form: Staff Service Request Form (and COT Entrance/Exit Form), COT-F181 Form
- Enterprise IT Form: Staff Service Request Form, EZ Version, COT-F181EZ Form
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule
- Kentucky Human Resource Information System (KHRIS)
- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- Kentucky Revised Statue (KRS) Chapter 61: House Bill 5 (HB5)
- National institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- OHRM Personnel Forms: Exiting Employees (for Supervisors) Checklist
- OHRM Personnel Procedures Handbook: Section 4.1- Disciplinary/Corrective Action
- Payment Card industry (PCI) data Security Standard (DSS) Requirements and Security Assessment Procedures Version 3.2.1
- Procurement, Payables, and Asset Tracking System (PPATS)
- Social Security Administration (SSA) Security Information
- U.S. Department of Education Family Educational Rights and Privacy Act (FERPA)